REMARKS

Applicants respectfully request reconsideration of the above referenced patent application in view of the amendments and remarks set forth herein, and respectfully request that the Examiner withdraw all rejections. No claims have been amended. No claims have been canceled. No claims have been added. Thus, claims 1-5, 7-33 and 35-38 are pending.

35 U.S.C. §103(a) Rejections

Claims 1-4, 11, 13-16, 18-20, 22, 24-27, 29 and 30-32

These claims are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Davis et al., US Pat. App. No. 2005/0076228 (hereinafter "*Davis*") in view of Ravi et al., US Pat. App. No. 2005/0204155 (hereinafter "*Ravi*") and Remer et al., USPN 7,076,653 (hereinafter "*Remer*") and Cromer et al., US Pat. App. No. 2005/0166213 (hereinafter "*Cromer*"). For at least the following reasons, Applicants traverse the above rejection.

Applicants respectfully submit that each of the above rejected claims is not obvious in light of *Davis, Ravi, Remer* and *Cromer*, based at least on the failure of the references to teach or suggest (emphasis added):

> "...prior to any allowing of the requested secure connection, **the embedded agent of the one of the clients verifying that a platform of the one of the clients is not in a compromised state** at a time before providing access to the encrypted traffic flow, and
>
> **in response to** the message requesting the secure connection and **the verifying**, the embedded agent of the one of the clients providing the key and an assertion that the one of the clients is not compromised to a verification entity on the network."

as variously recited in current independent claims 1, 11, 22 and 29.

Paragraphs [0038] and [0042] of *Davis* are cited in the claim rejection as allegedly teaching the variously claimed embedded agent of a client verifying, prior to any allowing of a requested secure connection, that a platform of the client is not in a compromised state. More particularly, the claim rejection relies upon a "smart card" authentication input device 136 allegedly being authenticated, and upon a security processing system 102 communicating information regarding an authentication status of the authentication input device 136.

Applicants note the distinction between an **authentication which is performed by** the authentication input device 136 in *Davis* and some alleged **authenticating of** the authentication input device 136 itself. Contrary to the assertions of the claim rejection, *Davis* fails to discuss any authenticating of the authentication input device 136. As described in *Davis*, the authentication input device 136 implements "the **authentication of a user** attempting to access host processor 130" (*Davis*, paragraph [0038], emphasis added) and/or the **authentication of security processing system 102** itself (see, e.g. *Davis* paragraph [0042]). However, *Davis* fails to provide any details as to whether or how authentication input device 136 itself might be authenticated.

It is authentication input device 136 which enables authentication for security processing system 102, and *Davis* fails to provide for security processing system 102 itself authenticating authentication input device 136. Therefore, any "information regarding an authentication status of the input device 136" (e.g. *Davis* paragraph [0042]) relates not to some authenticating of the authentication input device 136 itself, but rather to an authentication which is performed by authentication input device 136 – i.e. authentication of a user to security processing system 102 and/or authentication of security processing system 102 to some external network device. Therefore, contrary to the assertions of the Final Office Action, *Davis* fails to teach authenticating of the authentication input device 136, and also fails to teach verifying that a platform of a client is not in a compromised state, as variously recited in independent claims 1, 11, 22 and 29.

Even assuming *arguendo* that *Davis* discloses authentication of authentication input device 136, which Applicants do not agree, **merely authenticating an input device** – and/or communicating information regarding an authentication status of an input device – does not teach **verifying that a platform of a client is not in a compromised state**. By way of illustration, an input device may be compromised by malicious code, whereby the malicious code achieves access to use identification information (e.g. authentication credentials) of the input device. In such circumstances, the malicious code may then use such identification information **to correctly identify (e.g. authenticate) the input device as itself** to some other device/agent/entity – **despite the fact that the input device is in a compromised state**. In other words, such authenticating merely verifies that an input device is the same input device which it is purported to be. *Davis* fails to teach any authenticating which verifies, for example, that input device 136 (and/or security processing system 102) **is not in a compromised state**. This further demonstrates, in addition to other arguments set forth above, that *Davis* fails to teach verifying that a platform of a client is not in a compromised state, as variously recited in independent claims 1, 11, 22 and 29.

Response to Arguments Section

Applicants note that the *Response to Arguments* section of the Final Office Action also cites *Remer*, col. 10, lines 4-31 and *Cromer*, paragraphs [0048] and [0056] as allegedly teaching an embedded agent of a client verifying that a platform of the client is not in a compromised state. Applicants respectfully submit that such reliance on *Remer* and *Cromer* is unsupported, for at least the following reasons.

With regard to *Remer*, the relied-upon col. 10, lines 4-31 discusses establishing a secure connection with a LAN 230 after an authentication of a connection entity 10b of the LAN 230 with a trusted arbitrator 20b. However, as demonstrated above, **merely authenticating a device** (or entity) does not teach, for example, **verifying that some platform of a client is not in a compromised state**. Applicants note that *Remer* discusses authentication in terms of trusted arbitrator 20b verifying identification information, as opposed to verifying whether a platform is in a compromised state. See, e.g. *Remer* col. 4, lines 1-27. Accordingly, *Remer* col. 10, lines 4-31 verifies, at most, only that connection entity 10b (or trusted arbitrator 20b) is the same connection entity 10b (or trusted arbitrator 20b) which it is purported to be. However, any such verification in *Remer* of the identity of a connection entity 10b (or trusted arbitrator 20b) fails to address the question of whether some platform – e. g. a platform including identified connection entity 10b or trusted arbitrator 20b – might be in a compromised state.

With regard to *Cromer*, the relied-upon paragraphs [0048] and [0056] relate generally to a computer system 607 which includes a remote client 612 and a computer 605 operated as a troubleshooter for remote client 612. See, e.g. *Cromer* FIG. 6 and paragraph [0047]. The remote client 612 may be provided with what is described as "verification instructions 635" for remote client 612 to process modified wake-on LAN (WOL) packets from the troubleshooter – e.g. enabling logic for use of a public/private key algorithm and/or instructions for confirming an authorization of the troubleshooter. See, e.g. *Cromer* paragraphs [0023], [0048] and [0056]. However, in and of itself, **merely enabling remote client 612 to perform some task** – e.g. a public/private key algorithm or a confirmation of a remote troubleshooter's authorization – **fails to teach any verifying that remote client 612 is not in a compromised state**. Therefore, *Cromer* fails to indicate whether or how any such verification instructions 635 in *Cromer* might, for example, verify that some platform of remote client 612 is not in a compromised state.

For at least the foregoing reasons, *Davis*, *Remer* and *Cromer* all fail to teach verifying that a platform of the client is not in a compromised state. *Ravi* is not offered by the Final Office Action as curing – nor does *Ravi* cure – the failure of *Davis*, *Remer* and *Cromer* to teach the variously claimed verifying. By contrast, current independent claims 1, 11, 22 and 29 variously recite that, prior to any allowing of a requested secure connection, an embedded agent of a client verifies that a platform of the client is not in a compromised state at a time before providing access to an encrypted traffic flow.

Even assuming *arguendo* that all other limitations are obvious in view of *Davis*, *Ravi*, *Remer* and *Cromer*, which Applicants do not agree, the references nevertheless fail to teach or suggest at least one limitation of the invention as variously recited in each of independent claims 1, 11, 22 and 29. Accordingly, each of independent claims 1, 11, 22 and 29 is non-obvious in light of *Davis, Ravi, Remer* and *Cromer*, as are any claimed depending therefrom. For at least the foregoing reasons, Applicants request that the above 35 U.S.C. §103(a) rejection of claims 1-4, 11, 13-16, 18-20, 22, 24-27, 29 and 30-32 based on *Davis, Ravi, Remer* and *Cromer* be withdrawn.

Claims 5 and 33

These claims are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable in view of *Davis*, *Ravi*, *Remer*, *Cromer* and in further view of Yokota et al., US Pat. App. No. 2002/0164035 (hereinafter "*Yokota*"). For at least the following reasons, Applicants traverse the above rejection.

As demonstrated in the discussion above, there is at least one limitation in each of current independent claim 1, 11, 22 and 29 which is not taught or suggested by *Davis*, *Ravi*, *Remer* and *Cromer*. *Yokota*, which generally relates to the distribution and management of cryptographic keys, does not cure the failure of *Davis*, *Ravi*, *Remer* and *Cromer* to teach or suggest an embedded agent of a client verifying that a platform of the client is not in a compromised state. Therefore, even assuming *arguendo* that all other limitations are obvious in view of *Davis*, *Ravi*, *Remer*, *Cromer* and *Yokota*, which Applicants do not agree, the references nevertheless fail to teach or suggest at least one limitation of the invention as variously recited in each of independent claims 1, 11, 22 and 29.

Accordingly, each of independent claims 1, 11, 22 and 29 is non-obvious in light of *Davis*, *Ravi*, *Remer*, *Cromer* and *Yokota*, as are any claims depending therefrom. For at least the foregoing reasons, Applicants request that the above 35 U.S.C. §103(a) rejection of claims 5 and 33 based on *Davis*, *Ravi*, *Remer*, *Cromer* and *Yokota* be withdrawn.

Claims 9 and 37

These claims are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Davis*, *Ravi*, *Remer*, *Cromer* and in further view of Walker et al., US Pat. App. No. 2002/0163920 (hereinafter "*Walker*"). For at least the following reasons, Applicants traverse the above rejection.

As demonstrated in the discussion above, there is at least one limitation in each of current independent claim 1, 11, 22 and 29 which is not taught or suggested by *Davis*, *Ravi*, *Remer* and *Cromer*. *Walker*, which generally relates to techniques for routing packets according to a security association (SA), does not cure the failure of *Davis*, *Ravi*, *Remer* and *Cromer* to teach or suggest an embedded agent of a client verifying that a platform of the client is not in a compromised state. Therefore, even assuming *arguendo* that all other limitations are obvious in view of *Davis*, *Ravi*, *Remer*, *Cromer* and *Walker*, which Applicants do not agree, the references nevertheless fail to teach or suggest at least one limitation of the invention as variously recited in each of independent claims 1, 11, 22 and 29.

Accordingly, each of independent claims 1, 11, 22 and 29 is non-obvious in light of *Davis*, *Ravi*, *Remer*, *Cromer* and *Walker*, as are any claims depending therefrom. For at least the foregoing reasons, Applicants request that the above 35 U.S.C. §103(a) rejection of claims 9 and 37 based on *Davis*, *Ravi*, *Remer*, *Cromer* and *Walker* be withdrawn.

Claims 10, 17, 28 and 38

These claims are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Davis*, *Ravi*, *Remer*, *Cromer* and in further view of Ylonen, USPN 6,782,474 (hereinafter "*Ylonen*"). For at least the following reasons, Applicants traverse the above rejection.

As demonstrated in the discussion above, there is at least one limitation in each of current independent claim 1, 11, 22 and 29 which is not taught or suggested by *Davis*, *Ravi*, *Remer* and *Cromer*. *Ylonen*, which generally relates to network configuration using device-specific configuration packets, does not cure the failure of *Davis*, *Ravi*, *Remer* and *Cromer* to teach or suggest an embedded agent of a client verifying that a platform of the client is not in a compromised state. Therefore, even assuming *arguendo* that all other limitations are obvious in view of *Davis*, *Ravi*, *Remer*, *Cromer* and *Ylonen*, which Applicants do not agree, the references nevertheless fail to teach or suggest at least one limitation of the invention as variously recited in each of independent claims 1, 11, 22 and 29.

Accordingly, each of independent claims 1, 11, 22 and 29 is non-obvious in light of *Davis*, *Ravi*, *Remer*, *Cromer* and *Ylonen*, as are any claims depending therefrom. For at least the foregoing reasons, Applicants request that the above 35 U.S.C. §103(a) rejection of claims 10, 17, 28 and 38 based on *Davis*, *Ravi*, *Remer*, *Cromer* and *Ylonen* be withdrawn.

Claims 12 and 23

These claims are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Davis*, *Ravi*, *Remer*, *Cromer* and in further view of Grohoski et al., US Pat. App. No. 2004/0225885 (hereinafter "*Grohoski*"). For at least the following reasons, Applicants traverse the above rejection.

As demonstrated in the discussion above, there is at least one limitation in each of current independent claim 1, 11, 22 and 29 which is not taught or suggested by *Davis*, *Ravi*, *Remer* and *Cromer*. *Grohoski*, which generally relates to use of a cryptographic co-processor, does not cure the failure of *Davis*, *Ravi*, *Remer* and *Cromer* to teach or suggest an embedded agent of a client verifying that a platform of the client is not in a compromised state. Therefore, even assuming *arguendo* that all other limitations are obvious in view of *Davis*, *Ravi*, *Remer*, *Cromer* and *Grohoski*, which Applicants do not agree, the references nevertheless fail to teach or suggest at least one limitation of the invention as variously recited in each of independent claims 1, 11, 22 and 29.

Accordingly, each of independent claims 1, 11, 22 and 29 is non-obvious in light of *Davis*, *Ravi*, *Remer*, *Cromer* and *Grohoski*, as are any claims depending therefrom. For at least the foregoing reasons, Applicants request that the above 35 U.S.C. §103(a) rejection of claims 12 and 33 based on *Davis*, *Ravi*, *Remer*, *Cromer* and *Grohoski* be withdrawn.

Claim 21

This claims is rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Davis*, *Ravi*, *Remer*, *Cromer* and in further view of Kramer et al., US Pat. App. No. 2005/0201554 (hereinafter "*Kramer*"). For at least the following reasons, Applicants traverse the above rejection.

As demonstrated in the discussion above, there is at least one limitation in each of current independent claim 1, 11, 22 and 29 which is not taught or suggested by *Davis*, *Ravi*, *Remer* and *Cromer*. *Kramer*, which generally relates to encryption techniques using a cipher counter, does not cure the failure of *Davis*, *Ravi*, *Remer* and *Cromer* to teach or suggest an embedded agent of a client verifying that a platform of the client is not in a compromised state. Therefore, even assuming *arguendo* that all other limitations are obvious in view of *Davis*, *Ravi*, *Remer*, *Cromer* and *Kramer*, which Applicants do not agree, the references nevertheless fail to teach or suggest at least one limitation of the invention as variously recited in each of independent claims 1, 11, 22 and 29.

Accordingly, each of independent claims 1, 11, 22 and 29 is non-obvious in light of *Davis*, *Ravi*, *Remer*, *Cromer* and *Kramer*, as are any claims depending therefrom. For at least the foregoing reasons, Applicants request that the above 35 U.S.C. §103(a) rejection of claim 21 based on *Davis*, *Ravi*, *Remer*, *Cromer* and *Kramer* be withdrawn.

CONCLUSION

For at least the foregoing reasons, Applicants submit that the objections and rejections have been overcome. Therefore, claims 1-5, 7-33 and 35-38 are in condition for allowance and such action is earnestly solicited. The Examiner is respectfully requested to contact the undersigned by telephone if such contact would further the examination of the present application. Please charge any shortages and credit any overcharges to our Deposit Account number 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

Date: September 8, 2009

/Dermot G. Miller/
Dermot G. Miller
Attorney for Applicants
Reg. No. 58,309

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(503) 439-8778